Remarks

Claims 1-9, 12, 23-31, 33-43, 45-47 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 5,491,801 to Jain et al., U.S. Patent No. 6,820,128 to Firoiu et al. and U.S. Patent No. 6,643,292 to Chapman et al.; claims 3, 4, 9, 25, 26, 31, 37, 38 and 43 stand rejected under 35 U.S.C. § 103 as being unpatentable over the '801, '128 and '292 patents and U.S. Patent No. 6,646,987 to Qaddoura; claims 10, 32 and 44 stand rejected under 35 U.S.C. § 103 as being unpatentable over the '801, '128 and '292 patents and U.S. Patent No. 4,771,391 to Blasbalg; and claims 13-22 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,205,120 to Packer et al. in view of the '801, '128 and '292 patents.

Claim 1 recites:

> A method in a data processing system for managing traffic in a network data processing system, the method comprising:
> monitoring the traffic for a plurality of TCP connections or UDP associations through a given network path; and
> prior to sending a packet on a particular TCP connection or UDP association within the plurality of TCP connections or UDP associations, determining if the packet will cause the traffic for the network path to exceed a level of traffic allowed and, if the packet will cause the traffic for the network path to exceed the level of traffic allowed, reducing the traffic for one of the particular TCP connection or UDP association and another TCP connection or UDP association using an action based on a transmission protocol corresponding to the one TCP connection or UDP association.

Claims 13, 23 and 35 recite similar limitations.

Claim 7 recites:

> A method in a data processing system for managing traffic in a network data processing system, the method comprising:
> monitoring traffic for each of a plurality of TCP connections or UDP associations through a given network path; and
> prior to sending a packet on a selected TCP connection or UDP association within the plurality of TCP connections and UDP associations, determining if the packet will cause the traffic for the

> network path to exceed a threshold and, if the packet will cause the traffic for the network path to exceed the threshold, further determining if the packet will cause the traffic for the selected TCP connection or UDP association to exceed its fair share amount of the network path and if so, reducing the traffic for the selected TCP connection or UDP association using an action based on a transmission protocol corresponding to the selected TCP connection or UDP association.

Claims 18, 29 and 41 recite similar limitations.

As noted above, claims 1-9, 12, 23-31, 33-43, 45-47 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 5,491,801 to Jain et al., U.S. Patent No. 6,820,128 to Firoiu et al. and U.S. Patent No. 6,643,292 to Chapman et al.; claims 3, 4, 9, 25, 26, 31, 37, 38 and 43 stand rejected under 35 U.S.C. § 103 as being unpatentable over the '801, '128 and '292 patents and U.S. Patent No. 6,646,987 to Qaddoura; claims 10, 32 and 44 stand rejected under 35 U.S.C. § 103 as being unpatentable over the '801, '128 and '292 patents and U.S. Patent No. 4,771,391 to Blasbalg; and claims 13-22 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,205,120 to Packer et al. in view of the '801, '128 and '292 patents.

Jain et al. disclose in column 4, lines 52-62:

> a router determines the existence of an overload condition by detecting when it is operating beyond an estimated capacity level, it calculates a fair share of the estimated capacity level for each end system sending packets to the router and then, it identifies which end systems are sending more than a fair share of traffic received by the router. By conditioning a flag in the packets coming from the identified end systems, the router generates feedback indicating that the identified end systems are contributing to the overload condition in the router and that they should decrease their output.

Nowhere does Jain et al. disclose monitoring the traffic for a plurality of TCP connections or UDP associations through a given network path as required by independent claims 1, 13, 23 and 35 or monitoring traffic for each of a plurality of TCP connections or UDP associations through a given network path, as required by independent claims 7, 18, 29 and 41.

Rather, Jain et al. only teach monitoring the traffic passing through a router sent by a plurality of end systems.

The final Office Action states on page 3:

> Jain et al. further discloses prior to sending a packet determining if the packet will cause traffic for the network path to exceed the level of traffic allowed, and if so, reducing the traffic for the network path. **(See column 10, line 22 to column 11, line 39 ***)**

Jain et al. further disclose in column 10, lines 52-62:

> During periods of router overload, the router 9 sets the flag 21 on certain packets 13 in accordance with the approach described above. As a consequence, certain sources 7 will ultimately receive a sequence of packets some or all of whose flags 21 are set, thereby indicating that communications associated with that source are contributing to a stream of traffic which is accounting for more than a fair share of the limited capacity available at the router 9. The source 7 analyzes the sequence of congestion avoidance flags 21 which it receives to determine how to adjust its throughput.

Hence, Jain et al. teach, during periods of router overload, having the router set flags on certain packets, such that certain sources receive messages indicating that communications from each of those sources are contributing to a stream of traffic accounting for more than a fair share of the limited capacity of the router. Thus, in the Jain et al. system, a source has already sent communications exceeding its fair share of limited capacity of the router prior to the source learning of this condition. This is due to the fact that the condition is first detected downstream of the source by the router based on packets already sent by the source. Hence, Jain et al. do not teach detecting, prior to sending a packet, if the packet will cause traffic to exceed a level of traffic allowed. Rather, Jain et al. only teach that a source learns of an overload condition caused by packets it sent only after those packets have been sent.

Nowhere does Chapman et al. disclose, prior to sending a packet on a particular TCP connection or UDP association within a plurality of TCP connections or UDP associations, determining if the packet will cause the traffic for a network path to exceed a level of traffic

allowed, as required by independent claims 1, 13, 23 and 35, or prior to sending a packet on a selected TCP connection or UDP association within the plurality of TCP connections and UDP associations, determining if the packet will cause the traffic for a network path to exceed a threshold, as required by independent claims 7, 18, 29 and 41. Instead, Chapman et al. teach encapsulating one or more sets of customer data and sending the encapsulated data using conventional TCP algorithms using inherent TCP capabilities, see column 6, lines 58-61 and column 7, lines 18-30. Conventional TCP algorithms do not determine, prior to sending a packet on a particular TCP connection or UDP association within a plurality of TCP connections or UDP associations, if the packet will cause the traffic for a network path to exceed a level of traffic allowed. Conventional TCP algorithms also do not determine, prior to sending a packet on a selected TCP connection or UDP association within a plurality of TCP connections and UDP associations, if the packet will cause the traffic for the network path to exceed a threshold. Nor do Firoiu et al., Qaddoura or Blasbalg disclose, teach or suggest these aspects of the present invention.

There is absolutely no reason why one skilled in the art would combine the teachings of U.S. Patent No. 5,491,801 to Jain et al., U.S. Patent No. 6,820,128 to Firoiu et al. and U.S. Patent No. 6,643,292 to Chapman et al. in the manner set out in the final Office Action. Jain et al. is directed to monitoring the traffic passing through a router sent by a plurality of end systems. Firoiu et al. teach providing first and second buffers for storing different types of data, wherein the first and second buffers have different drop functions. Chapman et al. teach encapsulating one or more sets of customer data and sending the encapsulated data using conventional TCP algorithms using inherent TCP capabilities. Nowhere do these references disclose prior to sending a packet on a particular TCP connection or UDP association within a plurality of TCP connections or UDP associations, determining if the packet will cause the traffic for a network path to exceed a level of traffic allowed, as required by independent claims 1, 13, 23 and 35, or prior to sending a packet on a selected TCP connection or UDP association within the plurality of TCP connections and UDP associations, determining if the packet will cause the traffic for a network path to exceed a threshold, as required by independent claims 7, 18, 29 and 41. The

only teaching for the claimed subject matter comes from applicants' own disclosure, which cannot be used against them.

Accordingly, it is submitted that the Jain et al. patent, the Firoiu et al. patent, the Chapman et al. patent, the Qaddoura patent and the Blasbalg patent, whether taken singly or in combination, do not disclose, teach or suggest the subject matter set out in claims 1-10, 12 and 23-47.

As also noted above, claims 13-22 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,205,120 to Packer et al. in view of the '801, '128 and '292 patents. The Packer et al. patent lacks a teaching of monitoring the traffic for a plurality of TCP connections or UDP associations through a given network path as required by independent claim 13 or monitoring traffic for each of a plurality of TCP connections or UDP associations through a given network path, as required by independent claim 18. Nor do Jain et al. or Firoiu et al. teach this aspect of the present invention. Chapman et al. do not disclose, prior to sending a packet on a particular TCP connection or UDP association within the plurality of TCP connections or UDP associations, determining if the packet will cause the traffic for a network path to exceed a level of traffic allowed, as required by independent claim 13, or prior to sending a packet on a selected TCP connection or UDP association, determining if the packet will cause the traffic for a network path to exceed a threshold, as required by independent 18. Accordingly, it is submitted that the Packer et al. patent, the Jain et al. patent, the Firoiu et al. patent and the Chapman et al. patent, whether taken singly or in combination, do not disclose, teach or suggest the subject matter set out in claims 13-22.

It is also believed that claim 47 recites additional limitations which further distinguish it patentably from the applied prior art. Accordingly, it is submitted that claim 47 is patentable for this additional reason.

In view of the above remarks, applicants submit that claims 1-10 and 12-47 define patentably over the prior art. Early notification of allowable subject matter is respectfully requested.

Respectfully submitted,

Stevens & Showalter, L.L.P.

By /Robert L. Showalter/

Robert L. Showalter
Registration No. 33,579

7019 Corporate Way
Dayton, OH 45459-4238
Telephone: 937-438-6848
Fax: 937-438-2124
Email: rshowalter@sspatlaw.com

May 16, 2007